SAC065
SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
18 February 2014

Preface

This is an Advisory to the ICANN Board and community from the Security and Stability Advisory Committee (SSAC) on Distributed Denial of Service (DDoS) attacks leveraging Domain Name System (DNS) infrastructure. The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Advisory, references to SSAC members' biographies and disclosures of interest, and SSAC members' objections to the findings or recommendations in this Comment are at end of this Comment.

Table of Contents

Executive Summary

This document is intended for the Internet technical community, particularly authoritative and recursive Domain Name System (DNS) operators, network operators, the Internet Corporation for Assigned Names and Numbers (ICANN), and policy makers. It explores several *unresolved* critical design and deployment issues that have enabled increasingly large and severe Distributed Denial of Service (DDoS) attacks using the DNS. While DDoS attacks can exploit multiple characteristics of network infrastructure and operations, the prevalence and criticality of the DNS means that securing it is both challenging and urgent. These unresolved DNS issues and related DDoS attacks pose a real and present danger to the security and stability of the Internet.

The first recommendation below is made to ICANN, while others are made to operators of Internet infrastructure and manufacturers. While in many instances they reflect actions not under ICANN's control and actors not necessarily within ICANN's usual community, they are meant to address the overall responsibilities of the multi-stakeholder community and encourage ICANN to take action where it is relevant to do so. In particular, this means ICANN should be looking for ways to increase the effectiveness of steps already being taken against DNS abuse and promoting the participation of others as well as pursuing the measures suggested here.

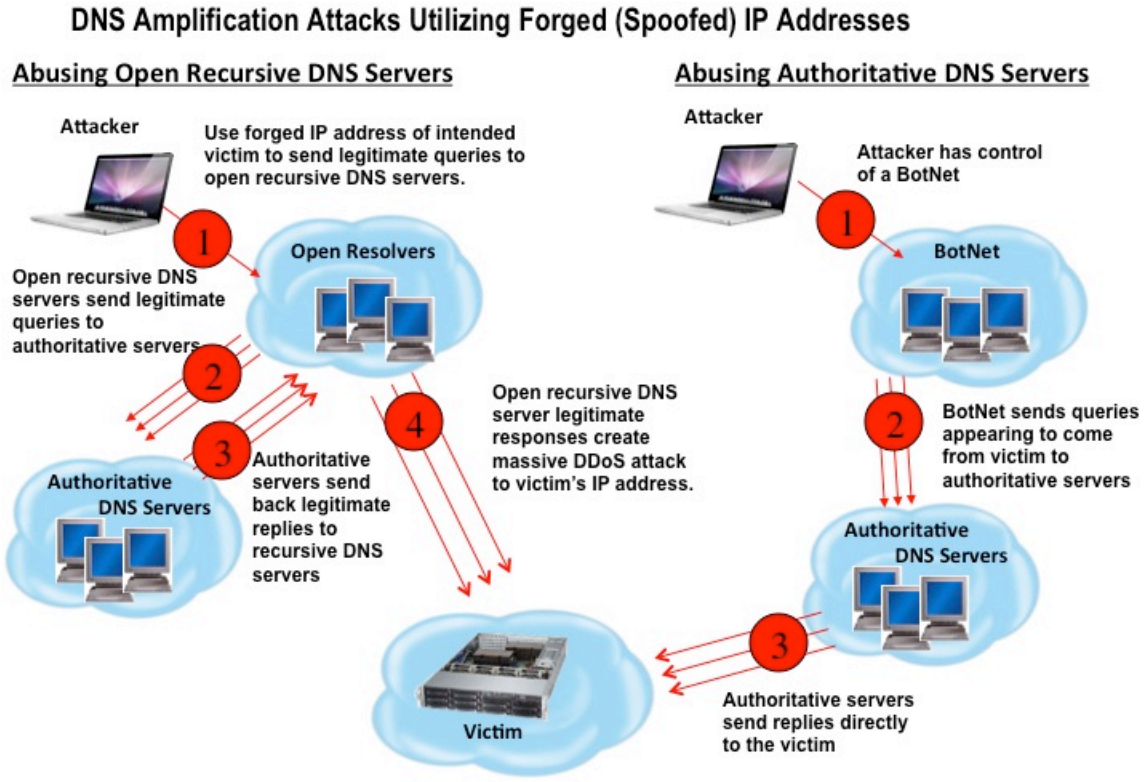
The Security and Stability Advisory Committee (SSAC) strongly recommends that *all* types of DNS operators and network operators take immediate steps to mitigate the design and deployment issues that make large scale DDoS attacks possible.

Specifically, the SSAC strongly recommends that:

1. ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow network spoofing. This effort should involve measurement efforts and outreach.
2. All network operators should take immediate steps to prevent network address spoofing.
3. Recursive DNS server operators should take immediate steps to secure open recursive DNS servers.
4. Authoritative DNS server operators should support efforts to investigate authoritative response rate limiting.
5. DNS server operators should put in place operational processes to ensure that their DNS software is regularly updated and communicate with their software vendors to keep abreast of the latest developments.
6. Manufacturers and/or configurators of customer premise networking equipment, including home networking equipment, should take immediate steps to secure these devices and ensure that they are field upgradable when new software is available to fix security vulnerabilities, and aggressively replace the installed base of non-upgradeable devices with upgradeable devices.

1. Introduction

Contemporary DDoS attacks use DNS reflection and amplification to achieve attack data bit rates reportedly exceeding 300 gigabits per second (Gbps).[1] Other recent attacks amplified by Simple Network Management Protocol (SNMP)[2] and Network Time Protocol (NTP) have resulted in attack bit rates exceeding 100 Gbps. Underlying many of these attacks is packet-level *source address forgery* or *spoofing*, a well-known vulnerability in which an attacker generates and transmits User Diagram Protocol (UDP) packets purporting to be from the victim's Internet Protocol (IP) address. Attackers often use query-response protocols (e.g., DNS or SNMP) to reflect and/or amplify responses to achieve attack data transfer rates exceeding the victim's network capacity either in bits per second, packets per second, or both. DNS is especially suitable for such attacks because the response is typically larger, and in some cases, much larger than the query. An example of two specific DNS amplification attacks is shown in the figure below.



In the attacks in which open recursive DNS servers are abused, the attackers generate queries with their source address forged to appear to have come from the IP address of

[1]See http://www.telegraph.co.uk/technology/internet-security/9957063/Web-slows-under-biggest-attack-ever.html and http://www.telegraph.co.uk/technology/internet-security/10022409/Spamhaus-attack-Dutchman-SK-arrested-in-Spain-for-biggest-ever-cyberattack.html.
[2]See http://www.bitag.org/report-snmp-ddos-attacks.php.

the victim (i.e., the attack target). As a result, responses are sent to the attack target. When such queries are distributed to even a moderate number of reflecting amplifying DNS servers, the result is a massive DDoS attack that is difficult or impossible for an attack target to mitigate.

In the attacks where authoritative DNS servers are abused, the attacker utilizes a botnet to generate queries directly to authoritative DNS servers. The queries have their source address forged to appear to have come from the IP address of the victim (i.e. the attack target). As with the previous attack, when such queries are distributed to even a moderate number of authoritative DNS servers, the result is a massive DDoS attack that is difficult or impossible for an attack target to mitigate.

These types of attacks have been observed to cause significant or total service outages for attack targets, as well as collateral damage to other systems. As network access speeds for users continue to increase, the aggregate power of such DDoS attacks will create extraordinary new attack data rates that will continue to outpace any reasonable capacity growth for attack targets. Since every Internet network and every Internet-connected device is a potential attack target, this problem is both compelling and urgent.

2. Why Is This Important?

Critically, basic controls for network access and DNS security have not been as widely implemented as is necessary to maintain and grow a resilient Internet. When increasingly higher-speed Internet connections are combined with the growing power of individual end user devices, an unintended result is an extraordinary and growing capacity for conducting extremely large scale and highly disruptive DDoS attacks using unsecured DNS infrastructure. Paradoxically, the networks that fail to implement the best current security practices are the sources, not the destinations, of attack data flows. Defenders are powerless to influence the design and implementation of the attackers' preferred networks. It takes only a relatively modest number of end-user devices, for example, to build or rent as a botnet for an attacker to generate significant attack traffic using only a very few, generally well-managed DNS authoritative servers operated by entirely innocent third parties.

These attacks have been growing in size over time, and are disrupting individual businesses;[3] entire networks, critical applications and services;[4] and entire countries.[5] The scale of attacks will continue to grow if the Internet community takes no further action.

3. Why Are These Attacks Possible?

There are many factors that contribute to the feasibility of these attacks:

[3]See http://www.independent.co.uk/news/uk/crime/anonymous-hackers-jailed-for-ddos-attacks-on-visa-mastercard-and-paypal-8465791.html.
[4]See http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers.
[5]See http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia.

- Many network operators have insufficient source address validation, which would prevent forgery of Internet packet source addresses.[6] The technical specification for how to validate source addresses has been available for decades, but not all operators have familiarity with those specifications or are able or willing to implement source address validation completely. In addition, vendor limitations of these functionalities have caused difficulties and impeded deployment of source address validation.
- Many network operators, and the community at large, have insufficient mechanisms to comprehensively measure and document the extent of source address validation. While attempts like the Spoofer Project[7] have attempted to measure the Internet's susceptibility to spoofed source address IP packets, the methodology doesn't take all network configurations into account. As a result, it is hard to (a) quantify the extent of compliance across the Internet and (b) contact non-compliant networks to improve compliance.
- Both DNS and its IP and UDP substrate evolved in an environment in which malevolent actors were not a significant concern and as a result, those protocols are almost ideal enablers for packet related attacks. DNS abuse can be accomplished through either authoritative or recursive name servers where the DNS queries are very small and the answers can be very large. Some authoritative name servers have begun to use a technique called response rate limiting (RRL)[8] to help this situation but more work is needed in this area.
- Many recursive DNS servers respond to queries from any source, rather than just sources within a specific network, sometimes as part of the vendor's default configuration of the device or software. As a result, many unmanaged open recursive DNS servers are being leveraged to amplify and reflect DDoS attacks. This lack of source limitation includes DNS servers in large hosting centers, Internet Service Provider (ISP) networks, enterprise networks, and home (residential end user) networks.
- While some community efforts have been undertaken to comprehensively and consistently measure the prevalence of open recursive DNS servers,[9] those efforts have lacked scientific due-diligence and are continually undergoing improvements. As a result, it is hard to (a) quantify the extent of compliance with resolver best current practices[10] across the Internet and (b) contact non-compliant resolver operators and work with them to achieve compliance. Thus, the community should undertake formal Internet-wide measurement tools and a globally coordinated compliance program, coordinated by ICANN. This will require creating tools to consistently measure and document the types and extent of non-compliant systems.

[6] See http://www.bcp38.info/index.php/Main_Page.
[7] See http://spoofer.cmand.org.
[8] See https://kb.isc.org/article/AA-01000/0/A-Quick-Introduction-to-Response-Rate-Limiting.html.
[9] See http://openresolverproject.org.
[10] See http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2013/tr13-002-eng.aspx.

- Software bugs in Internet home gateway devices and other home networking gear generate massive numbers of junk queries sent to recursive DNS servers.[11] These junk queries can overload DNS servers, and can also cause DNS operators to respond to junk queries during times of attack when they should be responding to truly necessary queries.
- Internet infrastructure markets require backwards compatibility: When software bugs in networking equipment are identified, for example SNMP reflected amplification DDoS attack mitigation,[12] the current practice is merely to improve future versions of such equipment, with no impact on the extensive world wide installed base of existing equipment.

  The overall level of security in home networking equipment and software is low, which can allow attackers to leverage these devices in coordinated DDoS attacks. Worse, in many cases, it is not possible to upgrade these devices without physically replacing them.

For many of these issues, there is not only the direct damage to the victims to consider but also the collateral damage to the rest of the Internet. This includes congestion on network links shared by victims with other non-malicious users. The network operators who are not doing source address validation have very little if any attack-related costs. The costs they do incur may show up as added transit costs, and if the network operators are identified, they may face de-peering or other social sanctions. In addition, DDoS attacks hitting critical sites and services, from email to social media, can deprive hundreds of millions of end users of access to these sites and services.

4. Prior Work on Mitigation Techniques

The problems listed above are not new. Over the years there have been a variety of standards, operational best practice documents, and regulatory audit requirements that have tried to address many of the issues. In this section, we provide a brief overview of prior work on mitigation techniques. Additional resources, which include user guides and detailed technical explanations, are listed in the Appendix below.

4.1 IP Source Address Forgery

Unless network operators take steps to prevent network address spoofing, the forging of source addresses in packets that enables an attacker to cause traffic to be sent to someone else, these attacks will continue. Recommendations on the prevention of address spoofing can be found in BCP38 (RFC2827),[13] which was published in May 2000 as well as SAC004, which was published in October 2002.[14] Numerous vendor configuration guides exist, some of which are listed in the Appendix.

[11]See http://dns.comcast.net/index.php/entry/some-netgear-routers-causing-flood-of-dns-queries.
[12]See http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.
[13]See Request for Comments (RFC) 2827 at: http://tools.ietf.org/html/bcp38.
[14]See SAC004: Security the Edge (17 October 2002) at:
http://www.icann.org/en/groups/ssac/documents/sac-004-en.htm.

While anti-spoof filters can be created with simple inbound/outbound filtering rules, leading router vendors have created a feature called Unicast Reverse-Path Forwarding (uRPF) that can simplify some configurations. However, it should be recognized that there are some scenarios, such as Content Delivery Network (CDN) implementations, where source address modification under the same Autonomous System Numbers (AS) may be appropriate.

4.2 Open Recursive DNS Servers

Recursive DNS server operators must take steps to respond only to authorized hosts, such as those within a particular network, to avoid unintentional provision of recursive name service to the entire Internet. When combined with source address forgery, open access to a recursive server obfuscates the path back to the attacker, making DNS reflection and/or amplification attacks very hard to defend against.

Recommendations on restricting access to recursive DNS servers can be found in SAC008,[15] published in March 2006 as well as in BCP140 (RFC5358),[16] published in October 2008.

Some additional tactics that have been used in the more recent past include not answering for common amplification queries (e.g., ANY requests for isc.org or ripe.net)[17] and completely dropping requests for domains that have been identified as part of DNS amplification attacks utilizing techniques such as DNS Response Policy Zones (DNS RPZ)[18].

4.3 Authoritative DNS Servers

Under normal circumstances, authoritative servers must respond to all received queries regardless of source even if the source is not on the local network. Even though the servers are not the direct victim of the attacks, this utilizes Central Processing Unit (CPU) time and bandwidth from the authoritative servers and may cause denial of service.

Following general DNS architecture security best practices can mitigate many risks. Some authoritative name server vendors have implemented a technique called DNS Response Rate Limiting (DNS RRL) in their servers to reduce the number of responses being transmitted but further analysis and studies are needed to define widely useful solutions.

[15] See SAC008: DNS Distributed Denial of Service (DDoS) Attacks (31 March 2006) at: http://www.icann.org/en/groups/ssac/dns-ddos-advisory-31mar06-en.pdf.
[16] See Request for Comments (RFC) 5358 at: https://www.ietf.org/rfc/rfc5358.txt.
[17] http://isc.org/ and http://ripe.net/.
[18] See https://dnsrpz.info/.

4.4 Regulatory Compliance

In many regulatory compliance frameworks, policy statements exist for device hardening and access control. Some of the mitigation techniques described in this document have been represented in these policy statements and then realized in operational behavior. Thus, as part of the security policy that meets the compliance mandates, requirements to deploy the above-mentioned mitigation techniques should be added.

For example, some sections of the ISO27002 framework[19] discuss network access control. When policymakers define policies that adhere to the ISO27002 framework, ingress filtering and anti-spoof filters have been included as part of the policy language. From an operational perspective, these policies are then turned into operational realities to match with the compliance/audit mandate.

Similar documentation of appropriate configurations exist for the Payment Card Industry (PCI) and other international compliance mandates. Operators have utilized these mandates even if they are not specifically required to comply with them, as these documents contain detailed guidelines and practices that can help prevent misuse of the network both internally and by external parties.

5. Recent Attack Landscape

As the access network speeds that devices can utilize continue to grow, facilitated by thousands of virtual hosts with access to very fast networks, the amount of malicious traffic that can be generated in an attack is continually increasing. To give one example, network interface cards on servers have increased in speed from 10 Megabits per second (Mbps) to 100Mbps, 1Gbps, and 10Gbps. In many cases servers can have multiple 10Gbps interfaces today, and this is expected to increase to 100Gbps speeds (and beyond) within the next few years.

A similar trend for residential end users has been observed as users have gone from services that can utilize a few Kilobits per second (Kbps) to single digit Mbps, double and triple digit Mbps, and now 1Gbps in some cases. In the near future multi-hundred Mbps and 1Gbps services are expected to become commonplace. These trends are expected to continue for as long as Internet access speeds and end host computational power continue to increase, which means that the scope and power of attacks will continue to increase in the future.

These historical trends have led to a number of recent attacks that are of concern:

- A 2012 Broadband Internet Technical Advisory Group (BITAG) report on SNMP-based attacks noted in Section 2.4 that attacks in excess of 100 Gbps had been observed.[20]

[19] See http://www.27000.org/iso-27002.htm.
[20] See "SNMP-Reflected Amplification DDoS Attack Mitigation" August 2012 at: http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

- An organization was recently attacked[21] with peak traffic reaching over 300 Gbps. Three Internet exchange points were severely affected as well, which demonstrates how widespread collateral damage of these attacks can be.

In today's attack landscape, the attackers are taking note of remediation methods and are continually changing their tactics to create huge operational costs for the targets that are defending themselves against these large-scale attacks. Of even greater concern is the collateral damage to any Internet connectivity provider who may also suffer operational losses due to huge traffic surges throughout their infrastructures since they happen to be somewhere in the path to the intended victim and recipient of the DDoS attack.

Importantly, not all attacks utilize high bit rates. An effective attack might send a large number of small packets, overwhelming a victim's per-packet capacity without saturating per-bit capacity. Thus reflection is a first order problem, even in cases where amplification is not used. Both reflection and amplification are boons to an attacker, but for different reasons. The virtue of reflection is untraceability, whereas the virtue of amplification is efficiency. Defensive strategies must address both.

6. Recommendations

The SSAC directs its first recommendation below to ICANN, while others are directed to operators of Internet infrastructure and manufacturers. While in many instances these recommendations reflect actions not under ICANN's control and actors not necessarily within ICANN's usual community, they are meant to address the overall responsibilities of the multi-stakeholder community and encourage ICANN to take action where it is relevant to do so. In particular, this means ICANN should be looking for ways to increase the effectiveness of steps already being taken against DNS Abuse and promoting the participation of others as well as pursuing new measures suggested here.

The SSAC strongly recommends that *all* DNS operators and network operators take immediate steps to mitigate the design and deployment issues that make large scale DDoS attacks possible. "Network operators" here means any type of network: Internet Service Providers' networks, transit networks, Content Delivery Networks, enterprise networks, end user networks, virtual hosting providers, Application Service Providers, and more. "DNS operators" can include any party performing authoritative or recursive DNS server operations, from ICANN to generic Top Level Domains (gTLDs), country code TLDs (ccTLDs), registry and registrar operators, domain operators, ISPs, DNS Application Service Providers, and more.

All except the first recommendation are intended for any individual or organization that operates an Internet-connected network or any type of DNS server. A lack of action on these recommendations has and will have a profound effect on others in the Internet community; ICANN and policymakers around the world should be aware of these recommendations and work to support them.

[21] See http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho.

Specifically the SSAC strongly recommends that:

Recommendation 1: ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow network spoofing.

This effort should involve measurement efforts and outreach and cooperation in relevant technical fora involving network operators worldwide, but will not have an operational component. ICANN should support this effort with adequate staffing and funding. Such a program should cover at least the following topics:

a. Collect, create, and organize material that will assist in the implementation of recommendations 2-5 below. This would include:
    i. On an annual basis, publish and widely disseminate a report on the number and extent of open recursive DNS servers.
    ii. On an annual basis, publish and widely disseminate a report on the extent of networks that allow network spoofing.
    iii. Create and maintain an information portal with links to educational material, to be complemented by ICANN staff and community subject-matter expert contributions.
    iv. Inform how certain products (e.g., Computer Premises Equipment (CPE) devices) can play a significant role in DNS amplification attacks.
    v. Publish a regular (at least annual) advisory/report on the state-of-the art-mechanisms to identify or otherwise prevent amplification and reflection attacks, and ensure that such an advisory/report is widely disseminated in the Internet community.
    vi. Provide an annual report on the work accomplished.
b. Coordinate with the Internet community to popularize and support recommendations 2-5 below. This coordination should include exploration of whether operational requirements regarding open resolvers and the prevention of network spoofing can be incorporated into regulatory compliance frameworks and certification regimes.

Recommendation 2: All types of network operators should take immediate steps to prevent network address spoofing.

These steps involve:

a. Implementing network ingress filtering, as described in BCP38 and SAC004, to restrict packet-level forgery to the greatest extent possible; and
b. Disclosing the extent of their implementation of network ingress filtering to the Internet community as a means of encouraging broader and more effective use of ingress filtering.

Recommendation 3: Recursive DNS server operators should take immediate steps to secure open recursive DNS servers.

These steps involve:

a. Identifying unmanaged open recursive DNS servers operating in the network and taking immediate steps to restrict access to these servers in order to prevent abuse; and

b. Following SAC008 Recommendation 3 to (1) disable open recursion on name servers from external sources and (2) only accept DNS queries from trusted sources to assist in reducing amplification vectors for DNS DDoS attacks.

In addition:

c. DNS Application Service Providers should take all reasonable steps to prevent abusive use of their open resolvers so that they are not targets of abuse. This would include continuous monitoring for anomalous behavior**,** limiting or blocking known abuse queries (e.g., ripe.net ANY); tracking likely target victim IPs (attacks reported or addresses of heavily targeted servers) and restricting or disallowing responses to those IPs; and sharing information with similar operators to coordinate efforts to quell such attacks.

Recommendation 4: Authoritative DNS server operators should investigate deploying authoritative response rate limiting.

This involves:

a. Investigating mechanisms to deter DNS amplification attacks (e.g., Response Rate Limiting (RRL) in DNS server software), and implementing those that are appropriate for their environment;

b. Encouraging DNS software vendors to provide such capabilities; and

c. Frequently reviewing the state of the art of such mechanisms and update their environment as necessary.

Recommendation 5: DNS operators should put in place operational processes to ensure that their DNS software is regularly updated and communicate with their software vendors to keep abreast of latest developments.

This should minimally include:

a. Auditing and updating operational practices as necessary to ensure that a process is in place to systematically perform DNS software updates on both an on-going and an emergency basis; and

b. Encouraging DNS software vendors to implement and refine the relevant capabilities at reasonable cost in system resources.

Recommendation 6: Manufacturers and/or configurators of customer premise networking equipment, including home networking equipment, should take immediate steps to secure these devices and ensure that they are field upgradable when new software is available to fix security vulnerabilities, and aggressively replacing the installed base of non-upgradeable devices with upgradeable devices.

This minimally involves:

a. Ensuring that the default configuration on these devices does not implement an unmanaged open recursive DNS resolver;

b. Providing updates and patches for their equipment to keep the installed base of networking equipment up-to-date to address current security threats, or as a necessary alternative replacing non-updatable equipment with appropriately configured devices;

c. Ensuring that large-scale participants in purchasing of customer premise networking equipment (e.g., ISPs, government procurement, large enterprises) insist that networking equipment meet the standards discussed in this document.

7. Acknowledgments, Disclosures of Interests, and Objections and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Disclosures of Interest section points to the biographies of all Committee members and any conflicts of interest—-real, apparent, or potential—-that may bear on the material in this document. The Objections section provides a place for individual members to disagree with the content of this document or the process for preparing it. The Withdrawals section is a listing of individual members who have recused themselves from discussion of the topic. Except for members listed in the Objections and Withdrawals sections, this document has the consensus approval of all members of the Committee.

7.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this Report.

SSAC members

Jaap Akkerhuis
Roy Arends
Don Blumenthal
Ondrej Filip
Jim Galvin
Robert Guerra
Julie Hammer

Rodney Joffe
Merike Kaeo
Jason Livingood
Ram Mohan
Russ Mundy
Rod Rasmussen
Shinta Sato
Paul Vixie

ICANN staff

Barbara Roseman (editor)
Steve Sheng (editor)

7.2 Disclosures of Interests

SSAC member biographical information and Disclosures of Interests are available at: http://www.icann.org/en/groups/ssac/biographies-13feb14-en.htm.

7.3 Objections and Withdrawals

There were no objections or withdrawals.

Appendix: Additional Resources

Information Regarding uRPF Configurations

Unicast Reverse Path Forwarding (uRPF) is a security feature that enables a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network

Cisco:

- http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

Juniper:

- http://www.juniper.net/techpubs/en_US/junos12.2/topics/usage-guidelines/interfaces-configuring-unicast-rpf.html

H3C: S7500E:

- http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S7500E_Series_Switches/Configuration/Operation_Manual/H3C_S7500E_Series_OM(Release_6300_series_V1.03)/02-IP_Services_Volume/200912/658846_1285_0.htm

H3C S9500:

- http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S9500_Series_Switches/Configuration/Operation_Manual/H3C_S9500_OM-Release1648[v1.24]-IP_Services_Volume/200901/624708_1285_0.htm

Information on Closing Open Recursive Servers

Simple DNS Plus:

- http://support.simpledns.com/KB/a99/what-is-an-open-dns-server-and-how-do-i-fix-it.aspx

Windows Server 2008:

- http://technet.microsoft.com/en-us/library/cc771738.aspx

Cache recursion directions:

- http://www.team-cymru.org/Services/Resolvers/instructions.html

Open resolver project:

- http://openresolverproject.org

Information on DNS Server Security Best Practices

Secure Domain Name System (DNS) Deployment Guide

- http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf

Domain Name System (DNS) Security Reference Architecture

- http://www.dhs.gov/sites/default/files/publications/dns_reference_architecture_0.pdf

BIND 9 DNS Security

- http://www.nsa.gov/ia/_files/vtechrep/I733-004R-2010.pdf

On the Time Value of Security Features in DNS

- http://www.circleid.com/posts/20130913_on_the_time_value_of_security_features_in_dns/

DNS RRL – DNS Response Rate Limiting:

- Rate limiting Proposal by Paul Vixie and Vernon Schryver: http://www.redbarn.org/dns/ratelimits

Implementations

- NSD Response Rate Limiting: https://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/
- Knot Rate Limiting: https://www.knot-dns.cz
- BIND Rate Limiting: https://kb.isc.org/article/AA-01058
- Experience: DNS Rate Limiting a Hard Lesson, http://conference.apnic.net/__data/assets/pdf_file/0011/58880/130226.apops-dns-rate-limit_1361839670.pdf
- Comparison of RRL behaviour in BIND9, Knot DNS, and NSD https://indico.dns-oarc.net//contributionDisplay.py?contribId=1&confId=0
- RRL Measurements: http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf
- RRL Firewall setting: http://www.bortzmeyer.org/files/generate-netfilter-u32-dns-rule.py
- DNS RPZ – DNS Response Policy Zones: http://www.redbarn.org/dns/dnsfirewalls